What is claimed is:

1. A method comprising:

retrieving connection pairs from a connection table for a host that is attempting to gain access to another host;

determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously,

determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

2. The method of claim 1 wherein determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts.

3. The method of claim 1 determining other anomalies includes determining whether the connection request uses the transport control protocol (TCP).

4. The method of claim 3 determining other anomalies includes determining whether the connection requests use ports that are not well-known thus indicating a possible Trojan virus attack.

5. The method of claim 3 determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event.

6. The method of claim 1 wherein determining other anomalies includes determining whether the connection requests use ports that have not been used previously.

7. The method of claim 1 wherein determining other anomalies includes determining if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table.

8. The method of claim 1 further comprising:

determining whether conditions exist to decrease the severity assigned to an event.

9. The method of claim 8 wherein determining whether conditions exist to decrease the severity assigned to an event, comprises:

determining whether the hosts are in roles that commonly access each other's hosts.

10. The method of claim 8 wherein determining whether conditions exist to decrease the severity assigned to an event, comprises:

determining whether the host being connected to commonly receives connections from new hosts.

11. The method of claim 1 wherein determining if other anomalies in the connection patterns of each host exist further comprises:

determining whether conditions exist to decrease the severity assigned to an event; and if an event is still indicated,

sending an event warning message with a determined level of severity to an operator.

12. A computer program product residing on a computer readable medium for detecting unauthorized access in a computer network comprising instructions for causing a computing device to:

retrieve connection pairs from a connection table for a host that is attempting to gain access to another host;

determine whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously,

determine if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

13. The computer program product of claim 12 wherein instructions to determine other anomalies includes instructions to determine whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts.

14. The computer program product of claim 12 wherein instructions to determine other anomalies includes instructions to determine whether the connection request uses the transport control protocol (TCP).

15. The computer program product of claim 12 wherein instructions to determine other anomalies includes instructions to determine whether the connection requests use ports that are not well-known thus indicating a possible Trojan virus attack.

16. The computer program product of claim 12 wherein instructions to determine includes instructions to use heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event.

17. The computer program product of claim 12 wherein instructions to determine other anomalies includes instructions to determine whether the connection requests use ports that have not been used previously.

18. The computer program product of claim 12 wherein instructions to determine other anomalies includes instructions to determine if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table.

19. The computer program product of claim 12 further comprising instructions to:

determine whether conditions exist to decrease the severity assigned to an event.

20. The computer program product of claim 19 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether the hosts are in roles that commonly access each other's hosts.

21. The computer program product of claim 19 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether the host being connected to commonly receives connections from new hosts.

22. The computer program product of claim 19 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether conditions exist to decrease the severity assigned to an event; and if an event is still indicated,

send an event warning message with a determined level of severity to an operator.

23. Apparatus comprising:

a processing device;

a memory;

a computer readable medium storing a computer program product for detecting unauthorized access in a computer network comprising instructions for causing the device to:

retrieve connection pairs from a connection table for a host that is attempting to gain access to another host;

determine whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously,

determine if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

24. The apparatus of claim 23 wherein instructions to determine other anomalies includes instructions to determine whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts.

25. The apparatus of claim 23 wherein instructions to determine other anomalies includes instructions to determine whether the connection request uses the transport control protocol (TCP).

26. The apparatus of claim 23 wherein instructions to determine other anomalies includes instructions to determine whether the connection requests use ports that are not well-known thus indicating a possible Trojan virus attack.

27. The apparatus of claim 23 wherein instructions to determine includes instructions to use heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event.

28. The apparatus of claim 23 wherein instructions to determine other anomalies includes instructions to determine whether the connection requests use ports that have not been used previously.

29. The apparatus of claim 23 wherein instructions to determine other anomalies includes instructions to determine if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table.

30. The apparatus of claim 23 further comprising instructions to:

determine whether conditions exist to decrease the severity assigned to an event.

31. The apparatus of claim 30 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether the hosts are in roles that commonly access each other's hosts.

32. The apparatus of claim 30 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether the host being connected to commonly receives connections from new hosts.

33. The apparatus of claim 30 wherein instructions to determine whether conditions exist to decrease the severity assigned to an event, comprises instructions to:

determine whether conditions exist to decrease the severity assigned to an event; and if an event is still indicated,

send an event warning message with a determined level of severity to an operator.